State of Maine
Department of Administrative & Financial Services
Office of Information Technology

Access Control Policy and Procedures (AC-1)

Table of Contents

Table of Contents 2
1.0 Document Purpose: 3
2.0 Scope: 3
3.0 Policy Conflict: 3
4.0 Roles and Responsibilities: 3
5.0 Management Commitment: 4
6.0 Coordination Among Agency Entities: 4
7.0 Compliance: 4
8.0 Procedures: 4
9.0 Document History and Distribution: 11
10.0 Document Review: 11
11.0 Records Management: 11
12.0 Public Records Exceptions: 11
13.0 Definitions: 12

1.0 Document Purpose:

The purpose of this document is to define the State of Maine's policy and procedures to implement and maintain appropriate access controls for state *information assets*.

2.0 Scope:

2.1 This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1 Executive Branch Agency information assets, irrespective of location; and

2.1.2 Information assets from other State government branches that use the State network.

3.0 Policy Conflict:

If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0 Roles and Responsibilities:

4.1 **Agencies are responsible for:**

4.1.1 Ensuring that any contracts for vendor hosted/managed agency Information Assets adhere to any pertinent federal regulations, state regulations, and Office of Information Technology (OIT) policies, procedures, and standards.

4.1.2 Developing and implementing agency-level policy and procedures, to meet any additional, federal statutory requirements, pertinent to agency Information Asset access controls.

4.1.3 Ensuring that the access of any *authorized user* to agency Information Assets is based on the *principle of least privilege* and *separation of duties*.

4.1.4 Assigning an *agency data custodian* for agency information assets.

4.1.5 Developing and maintaining security plans for agency Information Assets.

4.2 **Office of Information Technology (OIT):**

4.2.1 **OIT is responsible for:**

4.2.1.1 Assigning an owner for each information asset supported by OIT.

4.2.2 **OIT Information Asset Owners are responsible for:**

4.2.2.1 Ensuring that any authorized personnel access to assigned assets is based on the principle of least privilege.

5.0 Management Commitment:

The State of Maine is committed to following this policy and the procedures that support it.

6.0 Coordination Among Agency Entities:

6.1 OIT coordinates with agencies to implement and maintain security controls, to safeguard agency information assets from unauthorized access from individuals or devices. Active Directory accounts are established through Help Desk or Footprint ticket requests.

6.2 Agencies work with their OIT application development managers, account managers, and the OIT Information Security Office to determine how access is managed and who, under what circumstances, may access agency information assets.

6.3 Application development managers serve as owners for the agency application systems that their teams support. Requests for application access go through the application development managers.

6.4 Access to particular parts of the network for administrative work is approved by the information asset owners.

7.0 Compliance:

7.1 For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline up to and including dismissal.

7.2 For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access and use State of Maine data and systems. Employers of non-State of Maine personnel will be notified of any violations.

7.3 Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement and the nature of the violation, penalties could include fines and/or criminal charges.

8.0 Procedures:

8.1 The following procedures serve as the base set of requirements for State of Maine information assets. They represent the security controls that have been established to provide an acceptable level of protection from unauthorized system access.

8.2 **Access Control Procedures for Users:**

8.2.1 User access control procedures are identified separately in Access Control Procedures for Users (AC-2)[1]. They include account management (AC-2), access enforcement (AC-3), separation of duties (AC-5), least privilege (AC-6), remote access (AC-17), wireless access (AC-18), and access control for mobile devices (AC-19).

8.3 **Information Flow Enforcement (AC-4):**

8.3.1 Agencies must ensure that agency Information Assets enforce approved authorizations for controlling the flow of information within the system and between interconnected systems, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.3.1.1 The flow of information traverses OIT-managed infrastructure assets (firewall, virtual private network (VPN), multi-layer switches, and router devices) that employ protocols that restrict Information Asset services.

8.3.1.2 The flow of information within systems and between systems is controlled in-part through OIT-managed firewalls, with rules that, by default, deny entry to all outside traffic to the state network.

8.3.1.2.1 Dedicated VPNs are also established, by OIT, in collaboration with external entities, to control the flow of information to/from approved foreign networks and cloud providers.

8.3.1.2.2 Demilitarized zones are implemented, by OIT, to limit inbound traffic to only information assets that provide authorized publicly accessible services, protocols, and ports. Inbound internet traffic is limited to IP addresses within the DMZ.

8.3.1.3 The flow of information within systems and between systems is controlled, in-part, through OIT-managed routers and multi-layer switches, which employ protocols to, by default, deny Information Asset access.

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/access-control-procedures-for-users.pdf

8.3.1.3.1 Access Control Lists (ACLs) are utilized to filter and control network traffic, and as the basis for flow control decisions.

8.3.1.3.2 Network diagrams that document Information Asset flow and interconnected systems on the State network are developed and maintained by OIT.

8.4 **Unsuccessful Logon Attempts (AC-7):**

8.4.1 Agencies must ensure that agency Information Assets enforce the following, with the number, time-period, and duration defined in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance:

8.4.1.1 A limit of (a defined number) of consecutive invalid login attempts by a user, during (a defined time-period); and that

8.4.1.2 The user is locked out of the account (for a defined duration) when the maximum number of login attempts is exceeded.

8.4.2 OIT enforces a limit of 3 consecutive invalid login attempts by a user (over any time period). Accounts are automatically locked for 15 minutes when the maximum number of login attempts is exceeded for Active Directory users.

8.4.2.1 These standards are enforced by group policy for all Active Directory users and extend to information assets that utilize Active Directory.

8.4.2.2 Agency information assets that do not leverage Active Directory must employ alternative mechanisms to ensure compliance with these standards.

8.5 **System Use Notification (AC-8):**

8.5.1 Agencies must ensure that a System Use Notification is displayed to users, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance,

8.5.1.1 OIT requires the display of an Acceptable Use of State Resources banner, that identifies usage considerations, for all local and remote State of Maine (SOM) domain users (Active Directory banner).

8.5.1.1.1 The State of Maine requires notice the system may contain Maine State and U.S. Government information,

the pornography restriction and the incidental use policy to be in the Active Directory banner.

8.5.1.1.2 The Active Directory banner remains displayed until the user acknowledges the usage conditions prior to SOM domain access being granted. Acknowledgment can be by clicking an OK button or by pressing enter.

8.5.1.1.3 Where required, OIT systems that do not use Active Directory will display a warning banner that contains the same content as the Active Directory banner.

8.5.1.2 Agencies define required banners, banner content, and user acknowledgement, for their agency Information Assets (including publicly accessible systems), and associated components, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.5.1.2.1 OIT asset owners implement, where technically possible, and to the extent possible, identified agency banners, banner content, and user acknowledgement.

8.5.1.2.2 This includes banners for end-users (e.g. business application users) and banners for privileged users (e.g., database, server, operating system, and network administrators).

8.6 **Concurrent Session Control (AC-10):**

8.6.1 Agencies must identify any required concurrent session controls for agency Information Asset end-users, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.7 **Session Lock (AC-11, including CE-1):**

8.7.1 Agencies must ensure that any required device lock controls for agency Information Assets are implemented, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.7.1.1 OIT initiates a device lock after fifteen (15) minutes of inactivity, or upon receiving a request from a user. This standard is enforced by group policy for all Active Directory users.

8.7.1.1.1 The device lock is maintained until the user reestablishes access, by providing their identification and authentication credentials.

8.7.2 Agencies must ensure that the Information Asset conceals, via the device lock, information previously visible on the display, with a publicly viewable image.

8.7.2.1 OIT implements a screen saver group policy for all Active Directory users, where the information previously visible on the screen is concealed and replaced with a publicly viewable image, when the device lock is activated.

8.8 **Session Termination (AC-12):**

8.8.1 Agencies must define session termination requirements, for their agency Information Assets, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.8.1.1 OIT implements user session termination at the information asset level. For example, SFTP, Unix, and network all have session termination controls in place, where all processes associated with a user's logical session (except processes specifically created by the user to continue after the session) are terminated after five (5) minutes of inactivity.

8.8.1.2 OIT application owners implement required agency-identified session termination controls at the application level.

8.9 **Permitted Actions Without Identification or Authentication (AC-14):**

8.9.1 Agencies must identify and appropriately document actions that can be performed on agency Information Assets and/or agency websites, without identification or authentication, consistent with organizational missions/business functions and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.9.2 The following do not currently require identification or authentication:

8.9.2.1 By statute, the Maine.gov portal is, by default, open to the public.

8.9.2.1.1 Depending on the sensitivity of content and functionality offered, agencies may elect to require authentication and/or identification for agency Information Assets and agency websites.

8.9.2.2 OIT manages three sets of publicly accessible devices: Department of Health and Human Services - My Maine Connection public devices, Maine State Library public devices, and Department of Labor Career Center public devices.

8.9.2.3 OIT does not verify phone calls. The State of Maine does not transact business based solely on caller identity.

8.10 **Use of External Information Assets (AC-20, including CE-1, CE-2, and CE-3)**:

8.10.1 Agencies must ensure that terms and conditions are established, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external Information Assets, allowing authorized individuals to:

8.10.1.1 Access the Information Asset from external Information Assets; and

8.10.1.2 Process, store, or transmit agency-controlled information, using external Information Assets.

8.10.1.3 OIT has a detailed Remote Hosting Policy[2] that establishes requirements and responsibilities for remote-hosted State of Maine Information Assets.

8.10.2 Agencies must permit authorized individuals to use an external Information Asset to access the Information Asset or to process, store, or transmit agency-controlled information only when the implementation of required security controls is verified, or approved Information Asset connection or processing agreements are in place, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.10.2.1 OIT has a detailed Remote Hosting Policy[2] that establishes default requirements and responsibilities for remote-hosted State of Maine Information Assets.

8.10.3 Agencies must restrict the use of agency-controlled portable storage devices by authorized individuals on external Information Assets, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/remote-hosting-policy.pdf

8.10.3.1 By default, OIT does not implement portable storage device restrictions, but has the capability to implement agency-defined restrictions for the information assets that OIT manages.

8.10.4 Agencies must restrict the use of non-organizationally owned information assets, or devices to process, store, or transmit agency information, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.10.4.1 The OIT Mobile Device Policy[3] prohibits State of Maine employees and contractors from connecting any new personal devices (e.g., not owned by the State of Maine or an approved vendor) to any State of Maine system for any reason (e.g., charging, data transfer, internet access).

8.11 Information Sharing (AC-21):

8.11.1 Agencies must ensure any information sharing includes protections consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8.11.2 Authorized users of a particular data type may only share data with other individuals, groups, and organizations authorized to receive that data type.

8.12 Publicly Accessible Content (AC-22):

8.12.1 Agencies must manage publicly accessible content by:

8.12.1.1 Designating personnel authorized to post information onto a publicly accessible agency Information Asset;

8.12.1.2 Training authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

8.12.1.3 Reviewing the proposed content of information prior to posting onto the publicly accessible Information Asset to ensure that nonpublic information is not included; and

8.12.1.4 Reviewing the content on the publicly accessible Information Asset for nonpublic information at agency-defined intervals and removing such information, if discovered.

8.12.2 Agencies designate webmasters and/or web coordinators to manage the publicly accessible content on their agency websites.

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/mobile-device-policy.pdf

8.12.2.1 Agencies authorize these individuals and InforME grants agency authorized access for agency personnel who manage publicly accessible content on the Maine.gov portal.

9.0 Document History and Distribution:

Version	Revision Log	Date
Version 1.0	*Initial Publication*	*August 19, 2019*

Approved by: Chief Information Officer, OIT.

Legal Citation: Title 5, Chapter 163: Office of Information Technology[4].

Waiver Process: See the Waiver Policy[5].

Distribution

This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (https://www.maine.gov/oit/policies-standards).

10.0 Document Review:

This document is to be reviewed annually and when substantive changes are made to policies, procedures or other authoritative regulations affecting this document.

11.0 Records Management:

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0 Public Records Exceptions:

Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

[4] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

13.0 Definitions:

13.1 **Access Control:** The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

13.2 **Agency Data Custodian:** Agency official, who, based on their position, is fiduciary owner of specific agency information assets. For instance, the Labor Bureau of Unemployment Compensation Director (or designee) is the Agency Data Custodian for Unemployment Compensation Information Assets, and the Health & Human Services Office of Family Independence Director (or designee) is the Agency Data Custodian for Benefits Information Assets.

13.3 **Authorized User**: An individual who has approved access to an Information Asset to perform job responsibilities.

13.4 **Information Assets**: The full spectrum of all Information Technology products, including business applications, system software, development tools, utilities, appliances, etc.

13.5 **Interconnection Security Agreements:** Specific agreements enforcing appropriate information security controls, instituted for any information exchange among agencies, and among external entities. These agreements outline the roles, responsibilities, and data ownership between the parties.

13.6 **Multi-Factor Authentication:** method by which the user is granted access after providing a minimum of two of the following; something they know (personal identification number, password, etc.), something they have (token, card, key, etc.) and something they are (biometric).

13.7 **Personal Devices:** Include the following categories:

13.7.1 Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory);

13.7.2 Portable computing and communication devices with information storage capability (e.g. notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices); and

13.7.3 Any other mobile computing device small enough to be easily carried by an individual, wirelessly transmit or receive information with local, non-removable data storage, and a self-contained power source.

13.8 **Personally Identifiable Information (PII)**: information which can be used to distinguish or trace the identity of an individual (e.g., name, social security

number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). Source: NIST CSRC Glossary[6]. Maine State law also has a more specific definition in 10 M.R.S. §1347[7].

13.9 **Principle of Least Privilege:** A security principle where users are assigned the minimal access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.

13.10 **Privileged User**: Users who are granted the rights that go beyond that of a typical business user to manage and maintain IT systems. Usually, these rights include administrative access to networks and/or devices. This does not include users with administrative access to their own workstation.

13.11 **Sensitive Information:** Information that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. Sensitive information may include PII and is protected against unwarranted disclosure and typically carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse (e.g., Federal Tax, Protected Health, Criminal Justice, or Social Security information). Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

13.12 **Separation of Duties:** A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud (i.e., no user should be given enough privileges to misuse the system on their own).

[6] https://csrc.nist.gov/glossary
[7] http://legislature.maine.gov/legis/statutes/10/title10sec1347.html